Голові разової спеціалізованої
вченої ради
Національного університету
«Львівська політехніка»
д.т.н., професору
Опірському Івану Романовичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора,
завідувача Спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Субача Ігоря Юрійовича
на дисертацію
Рудої Христини Степанівни
«УДОСКОНАЛЕННЯ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ГОЛОСОМ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ»
подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертації.

Дисертаційна робота Рудої Х.С. присвячена актуальній і важливій проблематиці забезпечення стійкості голосових біометричних систем в умовах інтенсивного розвитку штучного інтелекту та активізації нових кіберзагроз, спрямованих на персональні дані користувачів. Сучасні умови глобальної цифровізації, популяризація віддалених і безконтактних методів автентифікації, а також стрімке поширення мобільних і хмарних сервісів значно підвищують вимоги до надійності та безпеки методів ідентифікації людини за її голосом.

Особливу увагу заслуговує актуальність проблеми захисту голосових біометричних систем від атак із використанням генеративних технологій, що стало можливим завдяки стрімкому розвитку методів синтезу мовлення та автоматизованого клонування голосу. Поширення таких технологій серед широкого загалу знижує поріг входу для зловмисників, що підвищує ризик компрометації систем голосової автентифікації та вимагає термінового розроблення ефективних методів протидії.

Таким чином, дисертаційне дослідження є актуальним внеском у наукове забезпечення та практичну реалізацію безпечних технологій голосової

автентифікації, що відповідає глобальним викликам сучасного інформаційного суспільства та має високий потенціал для подальших прикладних розробок у галузі кібербезпеки та захисту персональних даних.

2. Аналіз змісту дисертаційної роботи

Дисертація Рудої Христини Степанівни є завершеною самостійною науково-дослідною працею, яка відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії. Робота складається зі вступу, чотирьох розділів основного змісту, висновків, списку використаної літератури та додатків. Загальний обсяг дисертації становить 162 сторінки.

У вступі обґрунтовано актуальність теми дослідження в контексті загроз, пов'язаних з розвитком технологій синтетичного мовлення, визначено мету, завдання, об'єкт і предмет дослідження, сформульовано наукову новизну, практичну значущість, а також наведено дані про апробацію та публікації.

Перший розділ присвячений огляду теоретичних засад побудови систем голосової автентифікації. Авторкою проаналізовано класичні, статистичні та нейромережеві підходи до обробки мовлення, охарактеризовано текстозалежні й текстонезалежні системи, а також визначено сучасні загрози, зумовлені поширенням технологій Voice Cloning і TTS. Підрозділ завершується формулюванням завдань дослідження.

У другому розділі подано концептуальну модель системи голосової автентифікації на основі нейромережевих трансформерів, яка поєднує класичну обробку сигналу з глибокими архітектурами (ECAPA, TitaNet, WavLM). Розглянуто основні етапи побудови системи — від збору та попередньої обробки сигналу до формування ембедінгів та верифікації. Проведено порівняння класичних та нейромережевих методів екстракції ознак і приділено увагу нормативно-правовим аспектам захисту біометричних даних.

Третій розділ містить опис реалізованої системи на основі голосових ембедінгів, включаючи модулі реєстрації користувачів, вибору метрик подібності та порогового налаштування. Здійснено експериментальне дослідження точності, продуктивності та масштабованості моделей. Запропоновано методику усереднення ембедінгів і продемонстровано стабільну роботу системи за наявності варіативності мовлення.

Четвертий розділ присвячено тестуванню стійкості системи до атак із використанням синтетичного мовлення. Авторкою згенеровано корпус фейкових аудіозразків за допомогою моделей RVC, XTTS, ElevenLabs, Tortoise. Проведено тестування у двох сценаріях (ідентичний та новий текст), а також оцінено ефективність детекції синтетичного мовлення. Розглянуто інтеграцію когнітивних факторів як додаткового рівня захисту.

У висновках систематизовано наукові й прикладні результати, наведено кількісні оцінки ефективності, а також сформульовано рекомендації щодо подальшого удосконалення архітектури систем біометричної автентифікації.

3. Наукова новизна основних результатів дисертації полягає у наступному:

1. Одержала подальший розвиток концепція удосконалення голосової автентифікації, в основу якої покладено широке і комплексне застосування на різних структурних рівнях технологій машинного навчання та штучного інтелекту з урахуванням міжнародних стандартів у сфері біометричної безпеки. Це створює методологічну основу до забезпечення стійкості системи в умовах зростаючих кіберзагроз, підвищення дискримінаційної здатності моделей у багатокористувацьких сценаріях та в реальних умовах застосування.

2. Удосконалено такі ключові структурні комоненти системи біометричної автентифікації як модулі порівняння, налаштування та реєстрації голосових зразків шляхом застосування нейромережевих і трансформерних голосових моделей і обґрунтованого вибору метричних функцій. Це збільшує інваріантність голосової автентифікації до міжсесійних варіацій та масштабування, а відтак підвищує достовірність верифікаційних рішень біометричної системи в умовах багатокористувацьких сценаріїв.

3. Вперше розроблено та застосовано методику оцінювання стійкості до атак із застосуванням синтетично згенерованого мовлення, зокрема на основі генеративних моделей (RVC, ElevenLabs, XTTS, Tortoise), що дозволяє верифікувати ефективність системи згідно з вимогами ISO/IEC 30107-3:2023 щодо тестування Presentation Attack Detection. Виявлено, що всі протестовані моделі демонструють вразливість до атак з застосуванням клонування голосу, що стало підставою для рекомендації впровадження детекторів синтетичного мовлення як обов'язкового компонента систем біометричної голосової автентифікації.

4. Розроблено емпіричну методику тестування стійкості системи до атак підміни із використанням синтетичних голосів, згенерованих моделями RVC, XTTS, ElevenLabs та Tortoise, що дозволяє верифікувати ефективність системи згідно з вимогами ISO/IEC 30107-3:2023 щодо тестування Presentation Attack Detection (PAD). Виявлено, що всі протестовані моделі демонструють вразливість до атак з застосуванням клонування голосу, що стало підставою для рекомендації впровадження детекторів синтетичного мовлення як обов'язкового компонента систем біометричної голосової автентифікації.

5. Вперше реалізовано та зіставлено підходи до виявлення синтетичного мовлення на основі генеративної моделі ElevenLabs і авторської моделі MFCC+SVM. Отримані результати покладено в основу рекомендацій

щодо впровадження універсальних антиспуфінгових механізмів у архітектуру голосових біометричних систем.

4. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Наукове значення дисертаційного дослідження полягає в розробленні та обґрунтуванні нового методичного підходу до побудови нейромережевих систем голосової автентифікації, стійких до сучасних генеративних атак із використанням синтетичних голосових зразків. Важливою особливістю роботи є інтеграція алгоритмів машинного навчання та нейронних мереж із класичними методами аналізу й обробки голосових сигналів, що дозволяє забезпечити високий рівень точності й надійності автентифікації користувачів навіть у складних акустичних умовах.

Запропоновані у дисертації рішення становлять інтерес для подальших наукових розробок у сфері інформаційної безпеки, штучного інтелекту, цифрової обробки сигналів і когнітивної біометрії. Окремої уваги заслуговують розроблені автором методики формування ембедінгів голосу, алгоритми виявлення синтетичного мовлення, а також результати експериментальної перевірки їх ефективності з використанням сучасних генеративних моделей, що підтверджує практичну значущість отриманих результатів.

Одержані наукові результати доцільно інтегрувати у зміст навчальних дисциплін, що охоплюють напрями інформаційної та кібернетичної безпеки, біометричної ідентифікації, цифрової обробки сигналів та даних, штучного інтелекту, нейронних мереж, прикладного програмування. Використання цих результатів у навчальному процесі сприятиме формуванню в студентів практичних компетентностей у створенні сучасних біометричних систем, що є актуальним для спеціальностей у галузях інформаційних технологій, комп'ютерних наук, кібербезпеки, програмної інженерії та системного аналізу.

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна. Результати, представлені у дисертаційній роботі, ґрунтуються на чітко визначених дослідницьких завданнях та ретельно підібраних методологічних підходах. Кожне наукове положення роботи логічно випливає з поставленої мети та базується на сучасному математичному і програмному апараті, що забезпечує системність у розробці та експериментальній перевірці моделей голосової автентифікації.

Особливістю дисертаційного дослідження є вдало реалізована інтеграція трьох наукових підходів — класичного підходу обробки мовних сигналів, глибинного нейромережевого навчання та методів детекції синтетичного мовлення, які було поєднано у комплексну модель автентифікації з

використанням ембедінгів голосу. Запропонована модель забезпечує високу точність ідентифікації користувачів та ефективно протистоїть генеративним атакам у реальних сценаріях, що підтверджує її наукову обґрунтованість та практичну цінність.

Експериментальний апарат роботи реалізований коректно та відповідає вимогам щодо проведення досліджень в області голосової біометрії. Отримані результати експериментів підтверджують точність, стабільність та відтворюваність розроблених моделей і методів, що свідчить про достовірність зроблених висновків. Новизна роботи полягає у створенні комплексного нейромережевого підходу до автентифікації за голосом, здатного ефективно функціонувати в умовах сучасних генеративних загроз та застосовуватись у прикладних задачах інформаційної безпеки в режимі реального часу.

6. **Практичне значення одержаних результатів** полягає у тому, що:

1. Розроблено та реалізовано архітектуру системи голосової автентифікації на основі вбудованих векторів, яка забезпечує відповідність принципам надійності, масштабованості та обмеження доступу до біометричних шаблонів, визначеним у ISO/IEC 24745:2022 та ISO/IEC 19795-1:2021. Впровадження архітектури в експериментальному середовищі дозволило досягти точності автентифікації до 96%.

2. Імплементовано модель виявлення синтетичного мовлення на основі MFCC+SVM, яка забезпечує точність виявлення атак до 89.75%, при цьому точність класифікації справжніх голосів залишається низькою (25.96%), що свідчить про потребу додаткових рішень. Модель відповідає вимогам ISO/IEC 30107-1:2023 до PAD-механізмів і рекомендована до застосування як додатковий рівень захисту в багатофакторних біометричних системах, що працюють із критичними даними.

3. Створено тестовий корпус голосових даних, за допомогою якого проведено порівняльне оцінювання ефективності мовних моделей у сценаріях підробки голосу з різним лінгвістичним наповненням.

4. Результати порівняльного тестування моделей TitaNet, ECAPA-TDNN, WavLM та PyAnnote можуть слугувати основою для обґрунтованого вибору архітектури в задачах біометричної автентифікації, орієнтованих на великомасштабні користувацькі бази. Зокрема, модель TitaNet продемонструвала найвищу стійкість до масштабування: збільшення числа зареєстрованих користувачів від 10 до 70 зумовило зниження точності в середньому на 3,55%. Оцінювання масштабованості здійснювалася згідно методологічних положень стандарту ISO/IEC 19795-2:2007, який регламентує сценарне тестування з варіативною чисельністю суб'єктів як одного з ключових параметрів експериментального дизайну.

5. Результати оцінювання ресурсної ефективності моделей TitaNet, ECAPA-TDNN та WavLM вказали на їхню придатність для розгортання на обчислювальних платформах з обмеженими ресурсами. Зокрема, модель WavLM-base-plus-sv забезпечує автентифікацію з точністю 93% витрачаючи на зіставлення голосових векторів в середньому 4.34 мс. Це означає, що модель, будучи заімплементованою на периферійних пристроях із обмеженими резурсами задовольняє вимоги до швидкодії, необхідної для роботи в реальному часі. Отримані результати відповідають критеріям ефективності, визначеними в ISO/IEC 29167-1:2014, та засвідчують можливість застосування таких моделей у вбудованих біометричних рішеннях, мобільних пристроях і системах контролю доступу.

7. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Рудої Христини викладено у чотирнадцяти наукових публікаціях, а саме: у восьми статтях (із них шість – у фахових наукових виданнях України та дві – у закордонних періодичних виданнях), розділі монографії і п'яти матеріалах наукових конференцій і семінарів. Особистий внесок авторки у колективні публікації полягав у розробленні методичних підходів, організації та проведенні експериментальних досліджень, а також у науковій інтерпретації та узагальненні отриманих результатів.

8. Оцінка структури дисертації, її мови та стилю викладення.

Структура дисертації є системною та відповідає всім встановленим Міністерством освіти і науки України вимогам до дисертаційних досліджень, що подаються на здобуття ступеня доктора філософії. Внутрішня побудова роботи демонструє послідовність та логічну узгодженість у висвітленні мети, поставлених завдань, обґрунтуванні використаної методології, представленні результатів і визначенні сфер їхнього практичного застосування.

Мова дисертації є грамотною, стилістично виваженою та відповідає академічним нормам. Виклад матеріалу характеризується чіткістю формулювань, логічністю аргументації та структурною впорядкованістю, завдяки чому текст легко сприймається і засвоюється. У роботі вдало застосовується сучасна наукова термінологія у сфері інформаційної безпеки, біометричних систем, цифрової обробки сигналів і машинного навчання.

У роботі відсутні порушення принципів академічної доброчесності. Використані літературні джерела та посилання оформлені належним чином із дотриманням вимог щодо цитування.

9. Зауваження та дискусійні положення щодо змісту дисертаційної роботи.

1) У першому розділі (підрозділ 1.4) детально аналізуються загрози генеративного типу, але в роботі не наведено достатнього аналізу можливостей і обмежень сучасних антиспуфінгових механізмів, які вже існують у відкритому доступі або комерційних рішеннях. На мою думку, такий порівняльний аналіз міг би додатково підтвердити актуальність запропонованих авторкою методик.

2) У другому розділі (підрозділ 2.5) описано застосування нейромережевих архітектур ECAPA-TDNN, TitaNet і WavLM, однак не наведено детального обґрунтування критеріїв вибору саме цих моделей серед інших наявних альтернатив (наприклад, ResNet, RawNet, x-vector тощо). Більш ґрунтовне пояснення такого вибору зробило б представлений підхід аргументованішим.

3) У третьому розділі (підрозділ 3.2) наведені метрики ефективності не супроводжуються аналізом похибок вимірювання та довірчих інтервалів для отриманих значень. Включення такої статистичної оцінки суттєво підвищило б переконливість отриманих результатів.

4) У четвертому розділі мало уваги приділено аналізу хибних спрацьовувань (False Acceptance), що виникали під час експериментів із синтетичними голосами. Було б корисно побачити детальніше пояснення причин таких випадків та рекомендації, яким чином мінімізувати ймовірність таких помилок.

5) У дисертації зустрічаються деякі термінологічні неточності. Наприклад, авторка стверджує, що дисертаційна робота присвячена вирішенню актуального науково-практичного завдання, хоча, на мою думку, згідно з постановою кабінету міністрів від 12.01.2022 р. №44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», нею вирішено конкретне наукове завдання, що має істотне значення для галузі знань інформаційні технології.

Водночас зазначені зауваження не зменшують наукової цінності та практичного значення роботи, є рекомендаційними й можуть бути використані авторкою для подальших досліджень і поглиблення результатів.

Висновок

Дисертаційна робота Рудої Христини Степанівни на тему «Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання» є завершеним самостійним науковим дослідженням, яке характеризується значущими науковими результатами та суттєвою практичною цінністю для сфери кібербезпеки. Зміст

і спрямованість дисертації повністю відповідають спеціальності 125 «Кібербезпека» та чинним вимогам Міністерства освіти і науки України щодо оформлення дисертаційних досліджень, а також положенням постанови Кабінету Міністрів України №44 від 12.01.2022 р. «Порядок присудження ступеня доктора філософії». Авторка дисертаційної роботи заслуговує на присудження їй ступеня доктора філософії.

Офіційний опонент
Завідувач Спеціальної кафедри №5
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
доктор технічних наук, професор Ігор СУБАЧ

Підпис Субача І.Ю. засвідчую.

Заступник начальника Інституту
(з наукової роботи)
кандидат технічних наук, доцент Сергій КОНЮШОК
«07» 08 2025 року